

LAWRENCE MATASAR, OSB #74209  
621 S.W. Morrison Street, Suite 1025  
Portland, OR 97205  
Tel: (503) 222-9830  
Fax: (503) 274-8575  
Email: [larry@pdxlaw.com](mailto:larry@pdxlaw.com)

STEVEN T. WAX, OSB No. 85012  
Federal Public Defender  
101 SW Main Street, Suite 1700  
Portland, OR 97204  
Tel: (503) 326-2123  
Fax: (503) 326-5524  
Email: [steve\\_wax@fd.org](mailto:steve_wax@fd.org)

Attorneys for Pirouz Sedaghaty

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF OREGON

|                                  |   |                      |
|----------------------------------|---|----------------------|
| <b>UNITED STATES OF AMERICA,</b> | ) | Case No. CR 05-60008 |
|                                  | ) |                      |
| Plaintiff,                       | ) | SUPPLEMENTAL MOTION  |
|                                  | ) | FOR CONTINUANCE      |
| vs.                              | ) |                      |
|                                  | ) |                      |
| <b>PIROUZ SEDAGHATY,</b>         | ) |                      |
|                                  | ) |                      |
| Defendants                       | ) |                      |

Defendant Pirouz Sedaghaty, by and through his attorneys, Lawrence Matasar and Federal Public Defender Steven T. Wax hereby replies to the government's response and provides additional information, specifically concerning electronic discovery, in support of his previously filed Motion for Continuance.

**Good Faith Efforts to Recover Data by the Defense**

The government's response suggests a significant disagreement between the parties over discovery. That is not generally the case. Mr. Sedaghaty recognizes that the government has exceeded its discovery obligations in many areas. Conversely, the

government has been clear from the outset of the case that it is not following its usual open file policy with respect to discovery. There is one significant area in dispute - the large amount of data recovered from ten computer hard drives seized from Mr. Sedaghaty. Regrettably, the manner in which that aspect of discovery has been handled is the reason why a continuance is required.

The defense has repeatedly requested that the government provide it with meaningful data from the drives that had been seized, examined and tested by the government's computer forensics experts. The defendant's requests were made, and are appropriate, under Fed.R.Crim.P. 16(a)(1)(E)(iii), which requires the government to permit the defendant to inspect and copy "books, papers, documents, data, photographs, tangible objects, buildings or places . . . if the item is within the government's possession, custody, or control and . . . the item was obtained from or belongs to the defendant," and under Fed.R.Crim.P. 16(a)(1)(F), which requires the government to permit the defendant to inspect and to copy the results or reports of any "physical or mental examination and of any scientific test or experiment."

The material at issue on the computer hard drives is not straightforward. One cannot simply plug the drives into a computer and read them. Many of the items from the computers that the government intends to use at trial are, rather, files that have been deleted, or were never saved to the drives, but exist on the computer because they were viewed on the internet. These items have been "recovered" from what is called "unallocated space." The recovery was the result of forensic work by government computer experts. Thus, the product of their recovery is the "result" or "report" of "any physical...examination" or "any scientific test or experiment" under Fed.R.Crim.P. 16(a)(1)(F). Thus, what the government is obligated to provide Mr. Sedaghaty is not

simply an image of the hard drives, but the data recovered from them as a result of the government's experts' work.<sup>1</sup>

As detailed in previous discovery pleadings and the motion for continuance, Mr. Sedaghaty sought a copy of the government's experts' work early on in the case. The government resisted these requests.

In May, 2008, when the government first provided the defense with the 10 computer hard drive images, the defense retained an expert whom they know to be an excellent computer forensics examiner. He has been employed in the computer business for over 20 years and has been employed as a computer forensics recovery examiner for 13 years. He has a nationwide reputation, working for on both civil and criminal cases. He has been retained by the Federal Public Defender for the District of Oregon more than 50 times in the last 10 years, and has been retained numerous times by other top Oregon defense attorneys. He has testified as an expert witness in federal and state courts in multiple jurisdictions. His diligent efforts are described at pages 3-5 of the Motion for Continuance. It should be noted that this type of computer recovery, particularly with regard to emails, is not automated, but requires a defense expert to use a manual approach, interacting with the forensic images and validating individual files.

Page 3 of defendant's previously filed Motion for Continuance details the defense efforts, in addition to the previously filed formal discovery motions, to obtain meaningful data from the drives. At this Court's November 12, 2008 discovery hearing, counsel described the basic dispute: the defense sought the result of the government's

---

<sup>1</sup> See, e.g., *United States v. O'Keefe*, 537 F.Supp.2d 14 (D.DC 2008), where the Court used the Federal Rules of Civil Procedure for guidance to determine that the government must provide electronically-stored information in a reasonably usable form.

hard drive analysis, such as emails and other files; the government provided image copies of the seized drives but refused to provide the actual emails and other files recovered from the drives. At the hearing, Mr. Wax stated: “if they have printouts of those e-mails, if they have a printout of the QuickBooks files that they have recovered from the computers, then it seems -- rather than putting us to the time and expense of attempting to duplicate that effort, they should provide it to us.” CM 188, 25-26. Mr. Cardani had previously stated, “We don’t think we need to do that,” CM 188, 23, and later concluded, “you know, we can only go so far in trying to do their work.” CM 188, 32.

Three months later, the defense expert was still unable to obtain meaningful data from the hard drives. On February 26, 2009, counsel and experts for both sides conducted a conference and telephone conference to assist the defense expert in his efforts. For some time after that conference, the defense believed it would be able to obtain the data in a useable format in time to prepare for trial. Therefore, even though he continued to believe that the government was obligated under Rule 16 to provide copies of what it had recovered, at a chambers conference on April 14, 2009 to discuss pending motions and a trial date, counsel for Mr. Sedaghaty advised the Court that while the defense “had asked previously for a ruling on the computer discovery issues, it appears as though we have that resolved. . . So in terms of our previous request to you to rule on the discovery of computer issues, I don’t think you need to attend to that today.” CR 190, 23-24. Unfortunately, counsel’s expectation that the defense would soon recover all necessary computer documents later proved to be incorrect.

After the February 26, 2009 conference with counsel and computer experts from both sides, the defense expert recovered a substantial amount of email material and

provided it to defense counsel on May 26, 2009. As the previously filed Motion for Continuance further describes, the analysis of this material, 39,000,000,000 bytes, requires substantial processing to obtain useful information. The defense retained additional experts to process and refine this material.

There are numerous computer forensics tasks that must be undertaken to effectively analyze the contents of the computers and prepare a trial defense. The vast majority of the main defense computer expert's available hours for this case have been used for a single task: to recover items already recovered by the government, thereby leaving defense counsel with insufficient time and resources to complete the remainder of the necessary analysis to make it useful to the defense in time for the currently scheduled trial date.

The tasks are numerous and complex. For example, different people had access to the computer drives and were able to sign on with different screen names. If an item the government seeks to introduce was read or produced by someone other than Mr. Sedaghaty, it may not be admissible against him. It is, therefore, necessary to determine whether this type of information can be recovered from the drives. As a second example, some of the exhibits are images of web sites. It is necessary to determine whether these images were saved on the computer by the person viewing the site or exist on the computer solely because they were viewed. As a third example, the date on which an item was viewed could also be relevant to its admissibility. As a fourth example, the defense team must now review material the government does not intend to use to determine whether it is exculpatory. The defense was not in a position to undertake any of these tasks without first recovering the items.

/ / /

**The government's witness list and exhibit list, received after the defense filed its motion for continuance, provide substantial additional reasons for a continuance in this case.**

On August 10, 2009, after the defense filed its Motion for Continuance, it received the government's Witness List and Exhibit List. Given that the Government's Exhibit List does not provide page numbers or other links to the discovery, the defense has not yet located many of the items. On August 14, 2009, the defense received a copy of a memorandum from government computer forensics expert Jeremy Christianson to IRS Special Agent Colleen Anderson. This memorandum contains a list of 264 Document Exhibit items and their location on the government drive images, 253 of which were recovered from unallocated hard drive space. It appears that the government has recovered material from the drives that the defense expert has not recovered, even with the guidance provided by the government. As a result, it is now necessary for the Court to address the electronic discovery issue that had previously been raised, but which was not resolved as had been expected. Mr. Sedaghaty hereby renews his request that the government be directed to provide him with the results of its computer forensic work on the hard drives.

Moreover, as indicated above, unallocated hard drive space consists of sectors of a hard drive that are no longer readable by its operating system. Such files can be recovered only manually, based on their sector locations, which is a time consuming process. It is estimated that the defense examiner, who has other trial obligations in other cases, will need three to four weeks of working days to recover these items. In addition, it will be necessary to review this resulting evidence to compare it with, and establish its relevance to, the computer evidence already recovered independently of  
 / / /

the government and to the approximately 60,000 page document collection the defense has already assembled.

## CONCLUSION

For the above stated reasons, the defense requests a continuance until May, 2010.

Respectfully submitted,

/s/ Lawrence Matasar  
LAWRENCE MATASAR, OSB No. 74209

/s/ Steven T. Wax  
STEVEN T. WAX, Federal Public Defender,  
OSB No. 85012